

Patient Data Security System Using Finger Vein Authentication

Akuwan Saleh¹, Anum Faticha M S²

¹Department of Electrical Engineering, Politeknik Elektronika Negeri Surabaya, Surabaya, Indonesia

²Data and Information Center, The General Elections Supervisory Board of the Republic of Indonesia, Jakarta, Indonesia

Abstract - The technology of using finger vein patterns is a biometric system that has a high level of security. By using the identification of blood vessels found on the human finger, when this data is needed it can be accessed immediately, and there is no possibility of being lost or forgotten. The condition of the blood vessels in the human body, precisely in the fat tissue, also makes it difficult for data to be stolen. A person's health data is quite crucial data. So we need a good security system. By using this blood vessel authentication, the data can only be accessed by the person concerned. With a finger vein pattern that is not easy to duplicate so it is suitable for creating a security system. In this research, we take advantage of the advantages of the finished vein pattern to create a patient data security system in the hospital. The system is made by utilizing one of the algorithms of an artificial neural network. This algorithm is oriented towards changing the value of weights and biases in the training process. From the training process, a model of an artificial neural network system is generated. The best labeling is for one finger vein identity, one label. The average time required for image recognition is 2.4 seconds. The best rejection result is 100% and the best acceptance is 81.67%.

Key Words: finger vein, health data, digital image processing, artificial neural network, security system

1. INTRODUCTION

Today, the protection of information technology is increasingly needed. In storing all kinds of existing information, a security system is needed that can ensure the preservation of that information. Likewise with the maintenance of health data information in hospitals. Based on the Regulation of the Minister of Health of the Republic of Indonesia No. 269 of 2008, only certain people can access health data or medical records owned by patients [1]. In its development, this data is stored digitally so that to access it, a special system is also needed that ensures the security of the data. Currently there are many security systems that are used as an identity that protects the information data. Security systems that have been widely used in the community include PINs, passwords and use biometric systems. Biometric systems use a unique method of recognizing one or more physical traits or patterns of human behavior. This pattern of human behavior is like handwriting, while human physical

characteristics can be seen based on physiological patterns such as irises, fingerprints and faces [2].

The security system using blood vessels and the iris is a technology that has a high level of security. However, the use of the iris has a greater disadvantage due to the use of light directly into the eye [3]. Meanwhile, using the blood vessels inside the finger is considered safer for human health. The veins are not visible because they are inside the finger. To duplicate data is almost impossible. So, in this final project, a health data security system will be created for patients with identification using blood vessels on the fingers.

The finger vein pattern is obtained by placing the finger between a NIR-LED (Near-Infrared Light Emitting Diode) and a CCD (Charge-Coupled Device) camera. The light produced by the NIR-LED will penetrate the finger and be absorbed by the hemoglobin. Infrared LED radiation has an electromagnetic spectrum with a longer wavelength than visible light. The resulting light beam is captured by a CCD camera so as to produce an image of the finger vein pattern [4]. The image will be processed using several image processing techniques and stored in the form of a matrix as a template in the database.

The stored image is processed by the preprocessing stage and the introduction stage. For the preprocessing stage using finger region localization, region of interest (ROI) segmentation, as well as improving the quality of the resulting image [5]. Furthermore, the data obtained will form an artificial neural network model that is used to identify new incoming data. So that the quality of the system can be known. The features of the image are taken using the Maximum Curvature Point algorithm which has a high level of reliability [6]. The artificial neural network will process the features that have been generated by the image in a Convolutional Neural Network structure [7].

1.1 Related Work

Research that has been carried out by Amran H, Saleh A and Tulus Y, discusses Implementasi finger vein recognition pada sistem keamanan brankas [10]. The finger vein pattern image is processed using the method integral projection with region-based axis projection algorithm to obtain a histogram of the finger vein pattern. Have successfully identified safe owners who performed finger vein scans on themselves with an average success

rate of 64% and rejected other users who performed finger vein scans against safe owners with a 100% success rate.

In the paper, Finger-vein biometric identification using convolutional neural network [7], written by Syafeeza Ahmad Radzi, Mohamed Khalil-Hani and Rabia Bakhteri, have proposed CNN is tested on a finger-vein database developed in-house that contains 50 subjects with 10 samples from each finger. An identification rate of 100% is achieved, with an 80/20 percent ratio for separation of training and test samples, respectively. An additional number of subjects have also been tested, in which for 81 subjects an accuracy of 99.38%.

2. SYSTEM OVERVIEW

The system in this research is divided into two processes as shown in Figure 1. The first process is to register the finger vein pattern of the user. The registered finger vein pattern will be saved. Finger vein patterns that have been stored, processed using image processing. The feature of the finger vein pattern is retrieved and registered as a user id. Each feature is then processed in an artificial neural network to get the value of bias and weight. To produce a model that is used for the recognition process. The second process is the finger vein pattern recognition process for user identification.

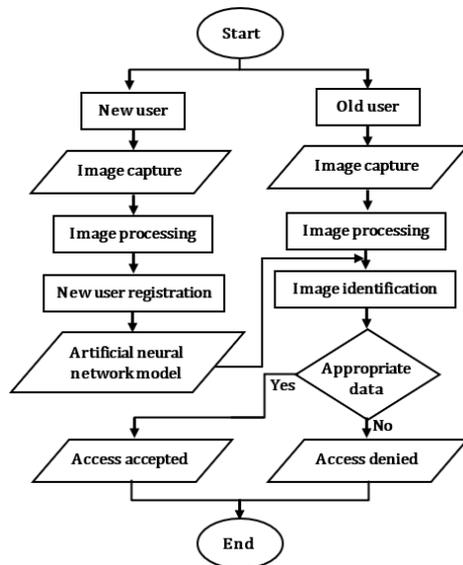


Fig -1: System flowchart

User ID is entered into the system. With the appropriate user ID, the camera will activate and start taking data in the form of an image of the finger vein pattern. The data received in the form of finger vein patterns were tested using a previously stored artificial neural network model. The vein pattern initially undergoes image processing first, then enters the authentication process with the model. If the data entered has a match with the model and with the appropriate accuracy value, then the incoming pattern is considered suitable, obtains access permission and can display the stored data. If they do not match, then the

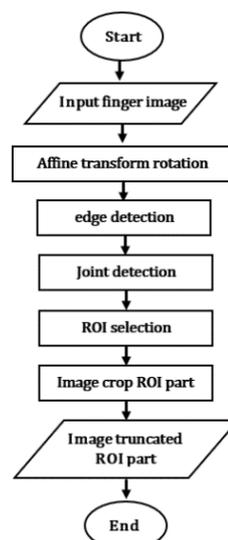
access permission will be denied and can not access the stored data.

2.1 Digital Image Processing

A digital image is a representation of image data or images in the form of a set of matrix data or digital values which are also called pixels (picture elements). Pixels are the main constituent of a digital image. Each pixel of the image carries 3 color combinations, namely red, green and blue which are commonly abbreviated as RGB (Red, Green, Blue). Sampling of digital image data is in the form of boxes that compose rows and columns. Each of these squares can be referred to as the data pixel. Basically an image consists of two dimensions that can be defined as a function $f(x,y)$, where x and y are spatial coordinates while the function f is the amplitude value in spatial coordinates (x,y) . When the x and y values and the light intensity value in the f function are not zero, it can be referred to as a digital image [8]. There are several types of file formats used, including files with the extension *.tif, *.png, *.jpg, *.gif, *.mpg, *.rgb and others [9].

2.1.1 Image Capture

The data taken is a finger vein pattern image capture using an infrared camera. The process of taking the image and the finger vein scanner is shown by the flowchart in Figure 2.



(a) flowchart (b) Finger vein scanner
Fig -2: Image capture

The finger vein pattern is then stored and used as a database that can be processed. The image that has been obtained is 640×480 pixels in size. The image obtained is normalized by rotating the image if the direction is not appropriate. The edges of the image are detected to make it easier to select the area to be processed further. The area taken for processing is the right edge and left edge of

the finger, as well as the upper and lower limits of the finger, namely the part between the joints [5]. The selected shape is a square, this area is known as the Region of Interest (ROI). The part that has been selected by the system is then cut according to the selected part.

2.1.2 Image Processing

The image that is processed for image processing is the final image of the image retrieval process. This image processing process is shown by the flowchart in Figure 3.

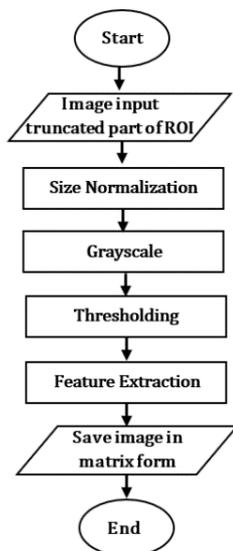


Fig -3: Image processing flowchart

The first process that is carried out is size normalization. In this process, the size of the image is changed. For example, an image that initially has a size of $I \times J$ pixels is then converted to a size of 240×120 pixels. The second process is an image that has been resized and then reprocessed into a gray color (grayscale). The third process, namely thresholding, is used to convert a grayscale image into an image with RGB values of 0 (white) and 255 (black) only. To get the Thresholding image, the gray level for each pixel is changed. For pixels with a gray level below 228, the color value is changed to 255. Meanwhile, if it is more or equal to 228, the color value is changed to 0. For pixels with an RGB value of 0, then it is coded with binary "1". As for pixels with an RGB value of 255, they are encoded with binary "0" and stored in the form of a matrix.

2.2 Finger Vein Authentication

Finger vein recognition is one of the biometric recognition technologies by utilizing the characteristics of the veins on the fingers. Finger vein patterns have unique and different characteristics on each person's finger. This difference can be used as an identification of the identity of each individual. This system is rated as a high security system. To duplicate the finger vein pattern is also difficult

because the finger vein pattern is below the skin surface and is not visible to the naked eye.

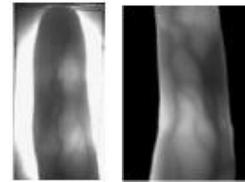
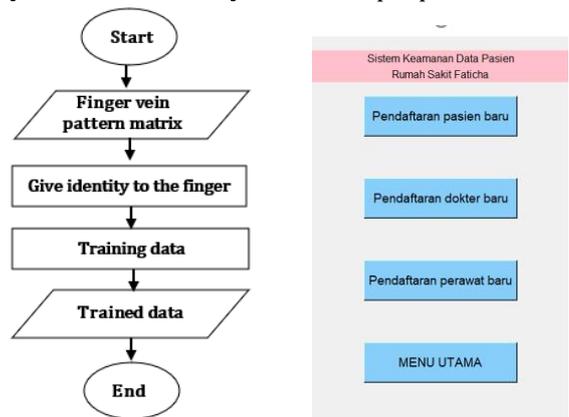


Fig -4: Finger vein pattern^[2]

How to get the existing finger vein pattern is by using infrared light. Venous blood vessels are located in fatty tissue close to human skin so they are easy to find with infrared devices. Then infrared rays are reflected on the camera so that the image of the vein pattern is captured [2].

2.3 New User Registration

New user registration is done to create a user database by storing user identities, finger vein pattern images and finger vein pattern matrix in the database. The database will contain 10 user identities. Each user identity can be used to access one registered patient data. Each user identity can be accessed by 5 different people.



(a) Flowchart (b) Display application

Fig -5: New user registration

In this case, the 5 people are like patients, 2 family members, 1 doctor and 1 nurse. These 5 different people will register their 4 fingers. Each finger is registered 5 times, assuming the registration position can change. The finished vein pattern matrix obtained is given an identity in the form of a label. Finger vein pattern matrix which is stored in the database which will later be used as train data for modeling the artificial neural network.

2.4 Artificial Neural Network

An artificial neural network is a branch of artificial intelligence. The basic concept of this artificial neural network is to imitate the workings of the human brain in processing various kinds of information. In the human

brain there are neurons that function as processors of incoming information data, in artificial neural networks there is also the term neuron as a processing unit. By referring to the working system of the brain, the artificial neural network makes a model of neurons with synapses or connections between neurons called weight (w), summed with the input value entered and the bias value (b), as well as the activation function (φ) which functions as a function. activation goes to the output section.

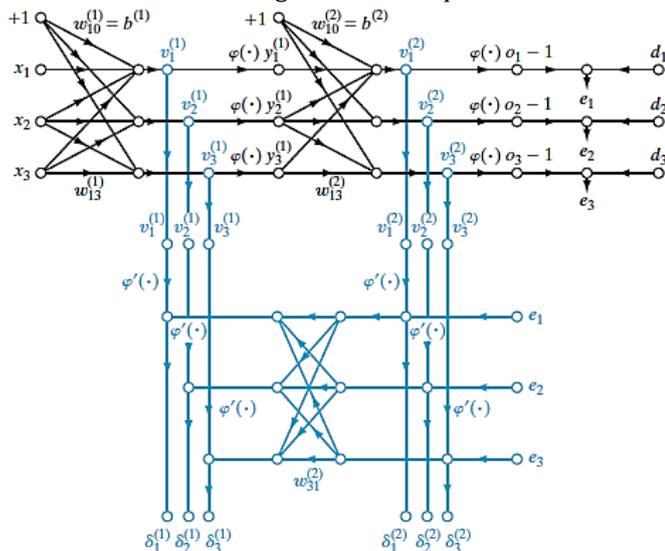


Fig -6: Backpropagation algorithm model illustration

Artificial neural networks have several types of learning such as supervised learning and unsupervised learning. One type of supervised learning that is commonly used is the backpropagation algorithm. This backpropagation algorithm is a learning system to update the model of the artificial neural network system. Starting with the feedforward process, then an update is made for the weight and bias values in the system. The update process is carried out backwards gradually on each neuron. There is a hidden layer in the system. The number of hidden layers and perceptrons/nodes in each layer affects the accuracy of the value between input and output. The number of iterations carried out also affects the change in the model and the level of value accuracy. In the backpropagation algorithm can be defined in several phases, initialization phase, forward computation, backward computation, and iteration. The initialization phase defines the weight value of the synapse with an empty value before the activation function.

From the illustration model can be explained further. The training data in this equation can be defined by the number of epochs written as $(x(n),d(n))$, with the input value of $x(n)$ being entered into the input layer. From layer l and neuron j generate $v_j^{(l)}(n)$ with the equation:

$$v_j^{(l)}(n) = \sum_i w_{ji}^{(l)}(n) y_i^{l-1}(n) \quad (1)$$

where $v_j^{(l)}(n)$ is the result of neuron i before layer $l-1$ in n iterations, and the value of $w_{ji}^{(l)}$ is the weight of neuron j layer l originating from neuron i in layer $l-1$. When $i = 0$ then the value of $y = 1$, and the value of $w = b$. Furthermore, if it is assumed to use the activation function, then the result of neuron j layer l is:

$$y_j^{(l)} = \varphi_j(v_j^{(l)}(n)) \quad (2)$$

If neuron j is located in the first hidden layer ($l=1$), then the equation is:

$$y_j^{(0)} = x_j(n) \quad (3)$$

If neuron j is located in the output layer ($l = L$, where L is the output layer), then the equation is:

$$y_j^{(L)} = o_j(n) \quad (4)$$

Error calculation can be formulated as:

$$e_j(n) = d_j(n) - o_j(n) \quad (5)$$

where $d_j(n)$ is the element of the j th neuron which is the response of the vector $d(n)$. Backward computation is the process of correcting and updating the values of w and b . In Figure 5. This process is depicted as a blue line. Defined local gradient (δ), expressed by the equation:

$$\delta_j^{(l)}(n) = \begin{cases} e_j^{(l)}(n) \varphi_j'(v_j^{(l)}(n)) \\ \varphi_j'(v_j^{(l)}(n)) \sum_k \delta_k^{(l+1)}(n) w_{kj}^{(l+1)}(n) \end{cases} \quad (6)$$

where the value of φ_j' is the sensitivity value. Update the value of w on layer l based on the delta rule, with an equation like:

$$w_{ji}^{(l)}(n+1) = w_{ji}^{(l)}(n) + \alpha [\Delta w_{ji}^{(l)}(n-1)] + \eta \delta_j^{(l)}(n) y_i^{(l-1)}(n) \quad (7)$$

where η is the learning-rate and is the momentum constant.

Activation function (φ) or activation function is used to pass the results to the next process. There are several types of activation functions that can be used in artificial neural networks, including hard-limit functions, log-sigmoid functions, linear functions and several other activation functions. The number of forward and backward computational iterations is determined by the number of epochs given or from the system that chooses when the iteration can be stopped. For image processing, a better artificial neural network method to use is CNN [8].

2.5 Artificial Neural Network Modeling

The finger vein pattern image matrix data is processed as train data or data used to form models. In the model created, the number of hidden layers is determined, the

activation function, the number of nodes or neurons in each hidden layer and the number of iterations required. Models that have been created are saved as files with the extension *.h5. In making an artificial neural network model, after going through the learning process, then the testing process is carried out.

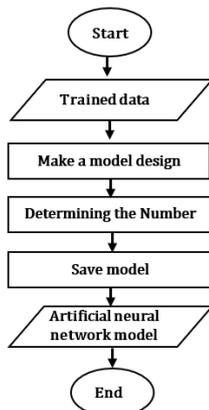


Fig -7: Flowchart of artificial neural network modeling

2.6 Image Recognition

Image recognition is done by re-entering the previously saved model. The way of image recognition is by taking an image of the finger vein pattern that will be recognized. Then it is predicted using the model that has been made. If the data matches the stored model, it will be allowed to access, otherwise it will be rejected.

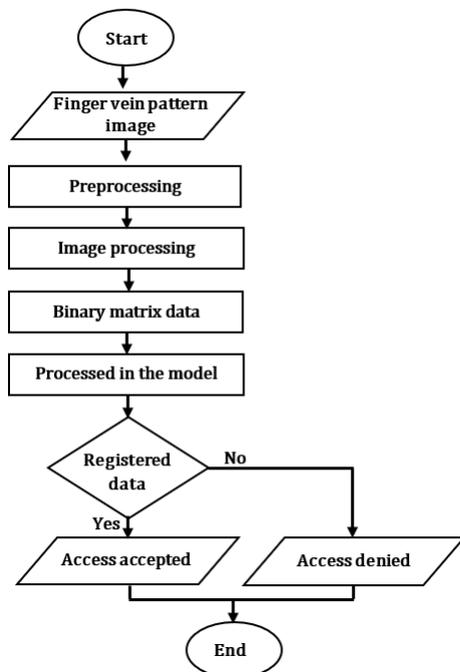


Fig -8: Image recognition system flowchart

2.7 Learning process

The resulting image in the form of image threshold data is then processed to enter into learning. The learning process is then stored as a datatrain. In this datatrain there are two things that are taken, namely features and labels. Learning data is stored in a file with the *.pickle extension. The data used for learning came from 5 people, namely 1 patient, 2 family members, 1 doctor and 1 nurse. Each person registers 4 fingers with each finger registered 5 times. This data is registered as 1 identity of the same patient. From this one data, it is then used as training data or learning data. The image obtained from each user who registers is taken 1 sample from each finger for image processing. The data after image processing will be used as training data to form the model.

Table -1: Process the patient's vein pattern image

Finger Name	Original Image	ROI	Grayscale	Threshold
Right index				
Left index				
Center right				
Middle left				

After obtaining the image of the finger vein pattern of each registered person, then the data is converted into training data.

```

0% | 0/21 [00:00<?, ?it/s] 10%|9 | 2/21 [00:00<00:01, 11.1
8it/s] 24%|#3 | 5/21 [00:00<00:01, 13.26it/s] 43%|####2 | 9/21 [00:
00<00:00, 16.17it/s] 62%|#####1 | 13/21 [00:00<00:00, 18.95it/s] 81%|#####
# | 17/21 [00:00<00:00, 21.67it/s] 95%|#####5 | 20/21 [00:00<00:00, 23.50i
t/s]100%|##### 21/21 [00:00<00:00, 25.50it/s]
0% | 0/21 [00:00<?, ?it/s] 24%|#3 | 5/21 [00:00<00:00, 43.2
0it/s] 43%|####2 | 9/21 [00:00<00:00, 39.78it/s] 62%|#####1 | 13/21 [00
:00<00:00, 37.74it/s] 81%|##### | 17/21 [00:00<00:00, 35.98it/s]100%|####
##### 21/21 [00:00<00:00, 35.25it/s]
0% | 0/21 [00:00<?, ?it/s] 24%|#3 | 5/21 [00:00<00:00, 42.4
6it/s] 43%|####2 | 9/21 [00:00<00:00, 39.00it/s] 62%|#####1 | 13/21 [00
:00<00:00, 36.93it/s] 81%|##### | 17/21 [00:00<00:00, 35.15it/s]100%|####
##### 21/21 [00:00<00:00, 34.70it/s]
0% | 0/21 [00:00<?, ?it/s] 24%|#3 | 5/21 [00:00<00:00, 43.9
8it/s] 43%|####2 | 9/21 [00:00<00:00, 40.11it/s] 62%|#####1 | 13/21 [00
:00<00:00, 37.73it/s] 81%|##### | 17/21 [00:00<00:00, 36.37it/s]100%|####
##### 21/21 [00:00<00:00, 35.62it/s]
0% | 0/21 [00:00<?, ?it/s] 19%|#9 | 4/21 [00:00<00:00, 34.2
8it/s] 38%|###8 | 8/21 [00:00<00:00, 33.67it/s] 62%|#####1 | 13/21 [00
:00<00:00, 35.60it/s] 81%|##### | 17/21 [00:00<00:00, 34.63it/s]100%|####
##### 21/21 [00:00<00:00, 34.52it/s]
100 data training
    
```

Fig -9: Data training process

In this training data, the features and labels of each image are taken. The features taken are in the form of binary data which is the result of feature extraction. The label that is taken is a class that is made to distinguish each person. In this case the data will be divided into 5 classes, patients, doctors, nurses, family members 1 and family members 2. The form of this class is an array, so the data will occupy positions 0, 1, 2, 3 and 4. The training data is stored as two files namely 'features.pickle' and 'label.pickle'. The stored training data is then processed to create a model.

3. RESULT

Tests were carried out using 2 different image sizes, namely 55×67 and 110×134 pixel. In testing this system there is a test scenario. There are 3 patient data that will be secured, namely Patient A, Patient B and Patient C. Patient A and Patient B are treated by the same doctor. Patient B and Patient C were treated by the same nurse. So that the data for Patient A is filled in by the finger vein pattern of the patient, 2 family members, 1 nurse and 1 doctor who is the same as Patient B. And for the data of Patient B and Patient C it is filled by the same 1 nurse. Thus, three models were produced, namely Model A for Patient A, Model B for Patient B and Model C for Patient C. The test was carried out at epochs 10, 20, 30, 40, 50 and a learning rate of 0.0001; 0.0002; 0.0003; 0.0004; 0.0005. The things that were tested were the duration of the model formation, the duration of identity recognition, and the accuracy of the match against the registered and unregistered data. Incoming data also undergoes an image processing process before being matched with existing data.

3.1 Image Size 55×67 pixel

There are 60 test data based on registered data and 40 test data based on unregistered data. Each classification of patient data is tested with an acceptance rate that varies, namely from an acc rate of 0.5; 0.6; 0.7 and 0.8. The results

for testing on Patient A for registered and unregistered data are as in Chart 1 and Chart 2.

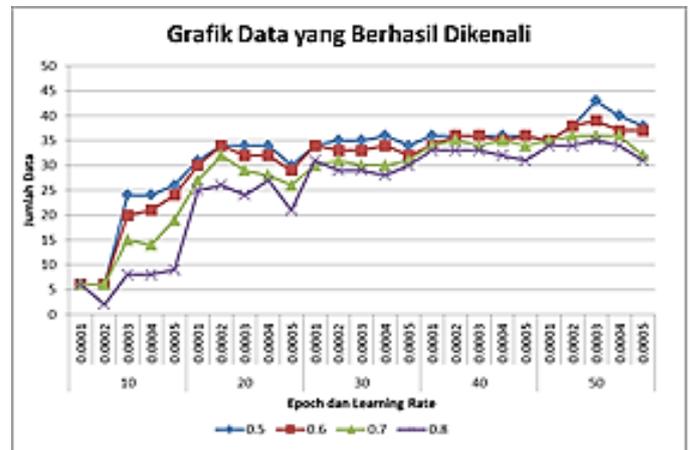


Chart -1: The data test graph has been recognized by model A image size 55×67

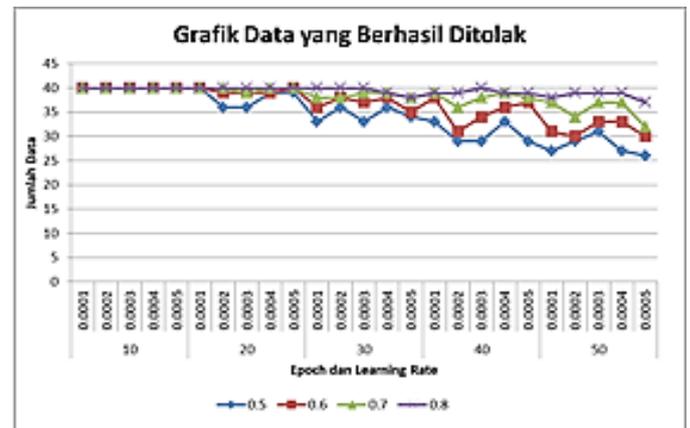


Chart -2: The data test graph was successfully rejected model A image size 55×67

Subsequent tests were carried out still with the same size, but using different data, namely for Patient B. The experimental results for Patient B data can be seen in the graphs of Chart 3 and Chart 4.

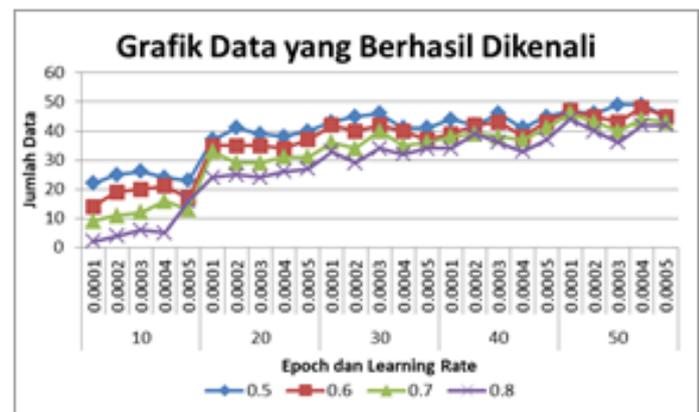


Chart -3: The data test graph has been recognized by model B, image size 55×67

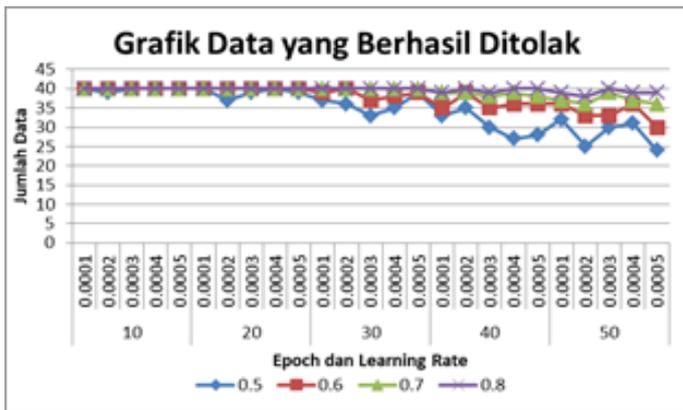


Chart -4: The data test graph was successfully rejected Model B image size 55×67

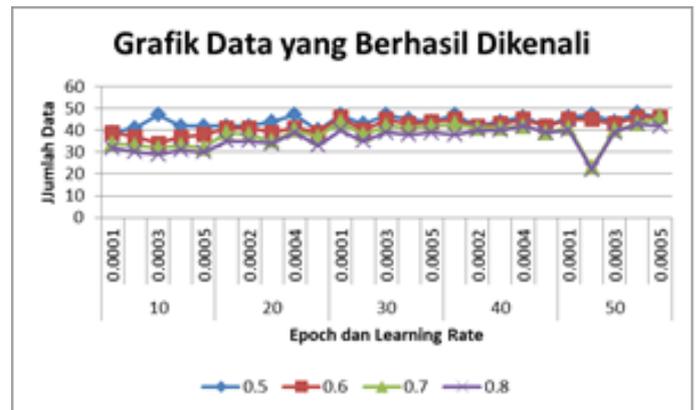


Chart -7: The data test graph has been recognized by model A image size 110×134

The experimental results for Patient C data can be seen in the graphs of Chart 5 and Chart 6.

There are 60 test data based on registered data and 40 test data based on unregistered data. Each classification of patient data is tested with an acceptance rate that varies, namely from an acc rate of 0.5; 0.6; 0.7 and 0.8.

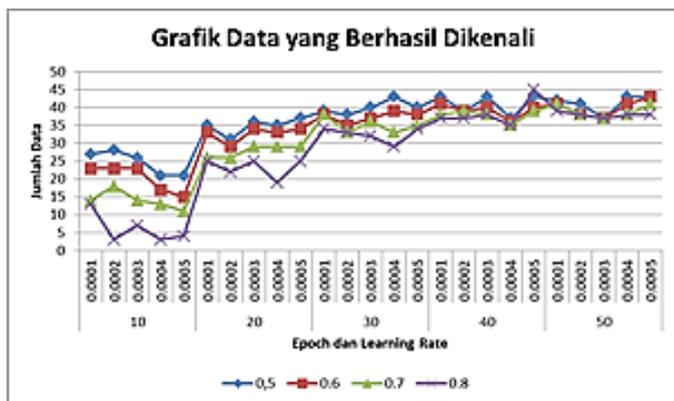


Chart -5: The data test graph has been recognized by model C image size 55×67

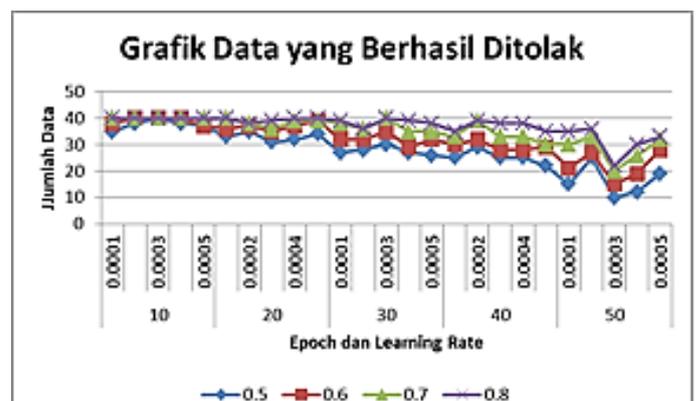


Chart -8: The data test graph was successfully rejected model A image size 110×134

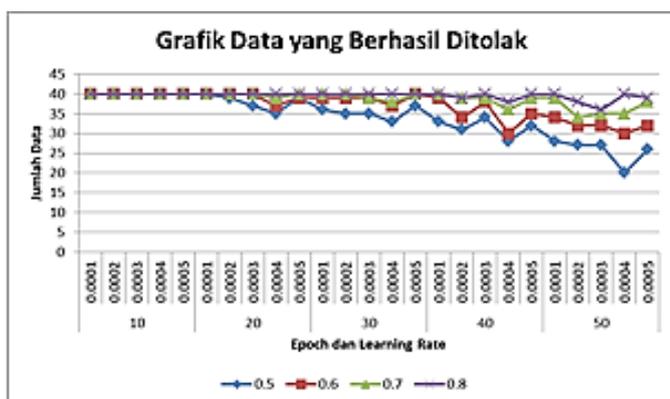


Chart -6: The data test graph was successfully rejected model C image size 55×67

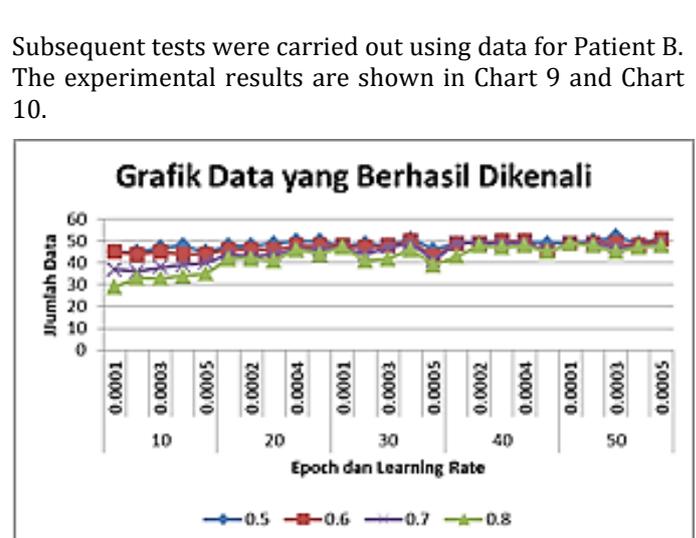


Chart -9: The data test graph has been recognized by model B, image size 110×134

3.2 Image Size 110×134 pixel

The results for testing on Patient A for registered and unregistered data are shown in Chart 7 and Chart 8.

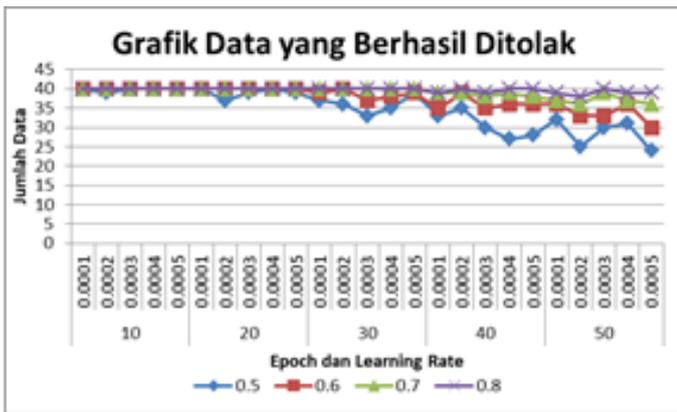


Chart -10: The data test graph was successfully rejected model B image size 110x134

The experimental results for Patient C data can be seen in Chart 11 and Chart 12.

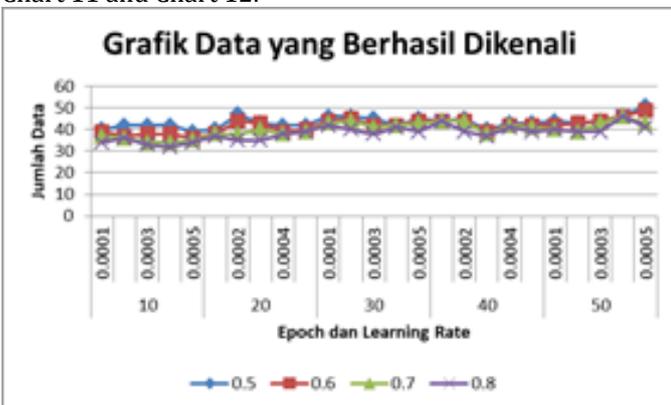


Chart -11: The data test graph has been recognized by model C, image size 110x134

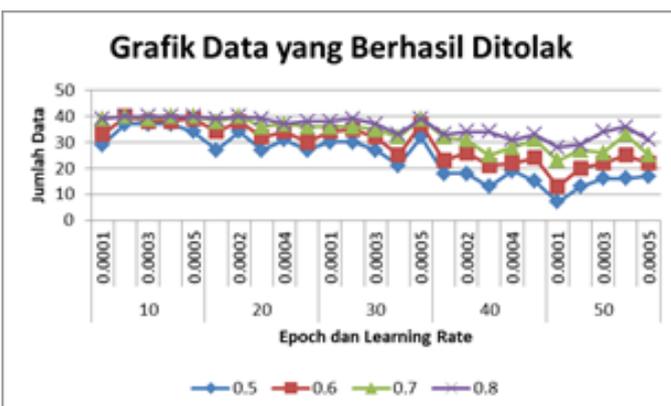


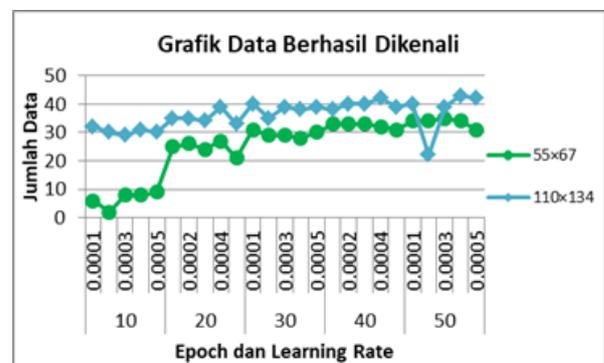
Chart -12: The data test graph was successfully rejected model C image size 110x134

The average recognition time of 5 times of testing with two different sizes, the results can be seen in Table 2. The data in table 2 shows the average recognition time required by this system, which is 2.4 seconds.

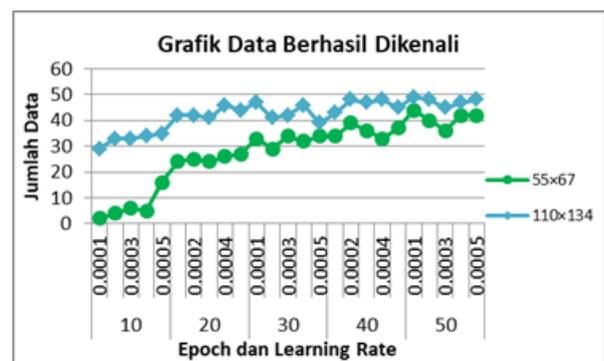
Table -2: Recognition time data with two different sizes

Test	Size 55x67 (s)	Size 110x134 (s)
1	2.77	2.12
2	2.64	1.59
3	2.5	2.29
4	1.96	2.8
5	2.49	2.76

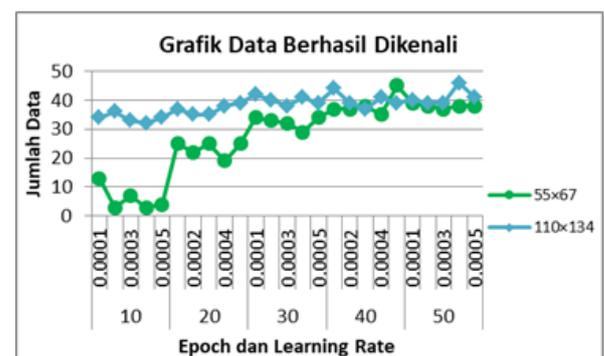
The results of epochs 10, 20, 30, 40 and 50 at a learning rate of 0.0001; 0.0002; 0.0003; 0.0004 and 0.0005 have the highest security at an acceptance rate of 0.8. From the 3 experimental models carried out, the results for registered data were successfully recognized as shown in Chart 13. For the results of the refusal test, the data is not registered as shown in and Chart 14.



(a)

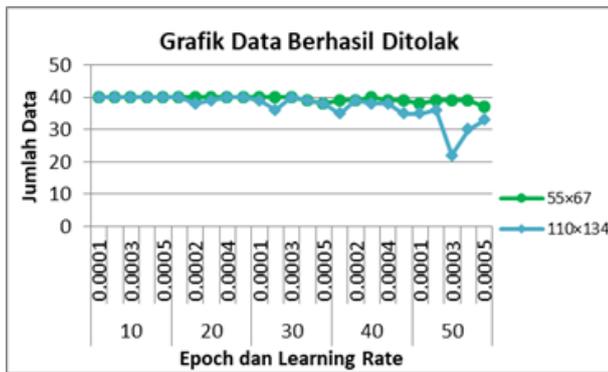


(b)

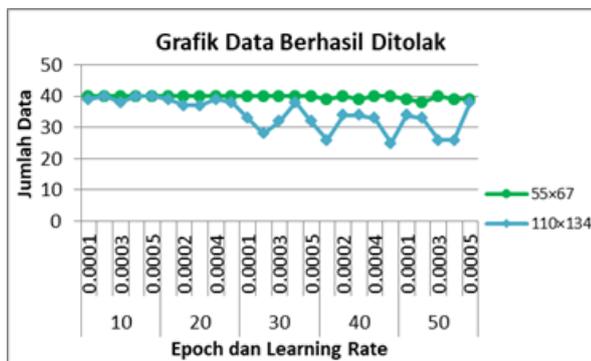


(c)

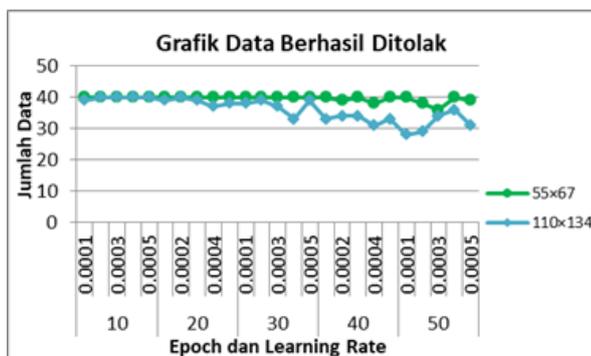
Chart -13: Graph of success in recognizing registered data (a) Model A, (b) Model B, (c) Model C



(a)



(b)



(c)

Chart -14: Graph of success rejecting unregistered data (a) Model A, (b) Model B, (c) Model C

From the three experiments on three different data groups, the average result was that the processed data with a size of 55x67 had a smaller success in receiving data than data that had a size of 110x134. The most recognizable number reached 49 data at a size of 110x134. While at the size of 55 x 67 the most number of recognizing data reaches 45.

As for the success of rejecting unregistered data, the average for data measuring 55x67 is higher than for data measuring 110x134. The number of identities that are recognized at the size of 110x134 unregistered data, then this can be caused because the unregistered data has the same features with the registered data. However, the best rejection percentage on both measures reached 100%.

Experimental results with various number of epochs and learning rates have been carried out. The results obtained for data measuring 55x67 have the best results at epoch 40 and epoch 50 with a learning rate of 0.0001-0.0005. For data measuring 110 x 134, the best results are in the number of epochs of 50 with a learning rate of 0.0001-0.0005.

4. CONCLUSIONS

From the results of the implementation of the system that has been made and the tests that have been carried out, it can be concluded that:

For data measuring 55x67, it has the best results at epoch 40 and epoch 50 with a learning rate of 0.0001-0.0005. The most stable results with a number of epochs of 40 and a learning rate of 0.0005. Data measuring 110x134 gets the best results in the number of epochs of 50 with a learning rate of 0.0001-0.0005. The most stable results with 50 epochs and a learning rate of 0.0001.

The system is able to identify data that has been registered correctly reaching 81.67%. Able to reject data that does not match the data that has been registered reaches 100%. The average time required for image recognition is 2.4 seconds.

ACKNOWLEDGEMENT

Finger vein scanner has been approved to be granted a patent by the Ministry of Law and Human Rights of the Republic of Indonesia Directorate General of Intellectual Property with the title Invention of Finger Vein Image Pattern Scanning Device. Notification No. HKI-3-HI.05.02.04. S00201911190-DP.

REFERENCES

- [1] Regulation of the Minister of Health of the Republic of Indonesia Number 269 of 2008 Chapter V Article 12.
- [2] K. Syazana-Itqan, A. R. Syafeeza, N. M. Saad, Norihan Abdul Hamid, dan Wira Hidayat Bin Mohd Saad, "A Review of Finger-Vein Biometrics Identification Approaches", Indian Journal of Science and Technology, 2016.
- [3] M. Mohamed Syed Ibrahim, Dr. Faris Salman Majeed Al Naimy, Dr. L. Rajaji, S.Syed Amma, "Biometric Recognition for safe Transaction using Vein Authentication System", Third International Conference on Sustainable Energy and Intelligent System, 2012
- [4] Jian Da Wu dan Chiung Tsiung Liu, "Finger-vein Pattern Identification using SVM and Neural Network Technique", ELSEVIER Expert System with Application, 2011.

- [5] Jia Liang Peng, Qiong Li, Ning Wang, Ahmed A. Abd El-Latif dan Xiamu Niu, "An Effective Preprocessing Method for Finger Vein Recognition", Fifth International Conference on Digital Image Processing, 2013
- [6] Naoto Miura, Akio Nagasaka, Takafumi Miyatake, "Extraction of Finger-Vein Patterns Using Maximum Curvature Points in Image Profiles", IAPR Conference on Machine Vision Applications, 2005.
- [7] Syafeeza Ahmad Radzi, Mohamed Khalil-Hani, Rabia Bakhteri, "Finger-vein Biometric Identification Using Convolutional Neural Network", Turkish Journal of Electrical Engineering & Computer Sciences, 2016.
- [8] Rafael Gonzalez, Digital Image Processing 3rd Edition, Pearson Hall: Upper Saddle River, 2008, pp. 1-103.
- [9] Tinku Acharya, Image Processing Principles and Applications, Wiley-Interscience: A John Wiley & Sons, Inc., Publication, 2005, pp. 1-428.
- [10] Amran H, Saleh A, and Tulus Y, "Implementasi Finger Vein Recognition pada Sistem Keamanan Brankas," Seminar Nasional Teknologi Elektro Terapan, Vol.02 No.01, ISSN: 2581-0049, Oct. 2018, pp. 147-152.

BIOGRAPHIES



The author is a graduate of master's education and currently works as a lecturer at Electronic Engineering Polytechnic Institute of Surabaya, in the city of Surabaya - East Java - Indonesia.



The author is a graduate of Bachelor of Applied and currently works as a Data and Information Center staff in the General Elections Supervisory Board of the Republic of Indonesia